

Consolidation Management Office
Adopt and Go - Analysis Summary

Vulnerability Management

Division

Security Management

Project Dates

October 1, 2005 to February 27, 2006

Scope

For purposes of this “Adopt and Go” project, Vulnerability Management is limited to the identification of vulnerabilities in the technology infrastructure and providing mitigation and remediation activities to minimize risk. A variety of subscription services are available that provide advisory notices that define specific hardware and software vulnerabilities, and provide mediation and remediation solutions. There are also products that continually probe the network for potential vulnerabilities and alert network managers to intrusion attacks in real time. Finally, testing a system’s vulnerabilities is commonly accomplished through third-party ethical penetration tests. Penetration testing, attempting to penetrate a systems security layers in order to demonstrate a security risk, requires skills not normally associated with data center resources. The subject “Adopt and Go Vulnerability Management Project” examines these issues and those dependent processes and activities necessary to support vulnerability oversight.

Adopted Processes

The Security Management Division has selected Symantec/DeepSight as the subscription product of choice for advisory services. Symantec is currently deployed at the Cannery Campus while the Gold Camp Campus subscribes to a number of products to provide advisory services. Symantec shall be deployed at the Gold Camp Campus as an “adopt and go” activity.

The Security Management Division has selected nCircle/IP360 Appliances as the key component for performing vulnerability assessment scanning and intrusion detection services. This software is currently deployed at the Cannery Campus. The software will be adopted at the Gold Camp Campus after it is confirmed that the IP360 Appliances can recognize all of the devices attached to the Gold Camp Campus. The Gold Camp Campus currently uses Internet Security Systems/Network Scanner software and the Cannery use Nessus software. Use of these software suites will be discontinued.

The Security Management Division has selected the Gold Camp Campus notification and remediation procedures (problem reporting and escalation) to support the nCircle/IP360

software. The Gold Camp Campus uses Remedy software to accomplish this function. The Cannery Campus will implement this procedure as an “adopt and go” activity.

The Security Management Division has elected to extend third-party penetration testing to the Cannery Campus. The Gold Camp Campus already engages in this activity.

The Gold Camp Campus will continue to provide Vulnerability Assessment Services to customers. This activity is outside the scope to this “Adopt and Go” project.